UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/669,452	09/24/2003	Mark L. Buer	50493/SDB/B600	4590

23363 7590 12/11/2007
CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
12/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/669,452	BUER ET AL.	
	Examiner	Art Unit	
	Farid Homayounmehr	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9 and 12-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/24/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application, filed 9/24/2003; amendment filed 9/24/2007.

2. Claims 1-9, 12-19 are pending in the case.

Response to Arguments

3. Applicants' arguments with respect to claim rejections have been fully considered, but they are not persuasive.

With regards to rejection under section 102, applicant argues: "Accordingly, Ziai does not teach or suggest "a shared input buffer associated with a plurality of input ports and the plurality of cryptographic processing cores, the shared input buffer configured to hold payload information associated with the data received by the plurality of input ports," as recited in amended independent claim 1 or "an input buffer shared among the plurality of input ports and the plurality of cryptographic processing cores," as recited in amended independent claim 12."

However, using plurality of input ports and plurality of cryptographic processing cores was well known at the time of invention. As indicated in the new grounds for rejection, Anand clearly teaches deploying multiple cryptographic processing cores as an option to increase the speed of cryptographic processing. Therefore, the combination of Anand and Ziai makes the invention obvious.

Note that in addition to teachings of Anand, Ziai's item 403 teaches "a shared input buffer associated a plurality of input ports". As shown in Fig. 4 and associated text, item 403 is clearly an input buffer. As shown in col. 7 lines 24-39, this buffer is a queue that packets waiting to be sent to the IPSec decryption accelerator are stored. Therefore all IP packets are headed for this buffer. As indicated in col. 4 lines 47-67 and/or col. 1 lines 48-60, Ziai's system works with both TCP and UDP protocol, as well as other transport protocols. TCP and UDP both run on top of the IP protocol, and have different ports. Therefore, the 403 buffer is shared as a packet queue for at least both the TCP and UDP packets. Therefore, item 403 is a shared input buffer associated a plurality of input ports.

Applicant further argues: Ziai does not teach: "a security association lookup unit configured to identify a security association address in a first portion of the address space associated with the cryptography accelerator by using header information, the first portion of the address space corresponding to bus controller memory." However, item 308 is a Security Policy Database (SPD), and item 309 is a Security Association

Database (SAD), which as described in the cited column 6, lines 17-43, determines the security policies associated with the received packet. The policy is looked up based on a reference provided by the SPD. As shown in col. 6 lines 4-17, the SPD is indexed according to packet header information. Therefore, the SPD and SAD lookup a security association for the packet based on the packet header information. To lookup data within a database, the address of the data must be identified. The SAD and SPD are associated with the decryption accelerator (cryptography accelerator), as shown in Fig. 4. Therefore, the identified security association is found in the address space associated with the cryptography accelerator. Also, Fig. 4 shows that the SAD, SPD and decryption accelerator are associated with the Direct Memory Access (DMA) Controller, item 410, which control and facilitates access to memory. Therefore, Ziai teaches a security association lookup unit configured to identify a security association address in a first portion of the address space associated with the cryptography accelerator by using header information, the first portion of the address space corresponding to bus controller memory.

Based on the discussion above, applicant's argument relative to allowability of claims 1-9 and 12-19 is found non persuasive.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-9 and 12-19 rejected under 35 U.S.C. 103(a) as being unpatentable over Ziai (US Patent No. 7,017,042, filed June 14, 2001), and further in view of Anand (U.S. Patent No. 7,266,703, filed Dec. 10, 2001)

5.1. As per claim 1, Ziai is directed to a cryptography accelerator (abstract, or items 402 or 411 in Fig. 4), comprising: a plurality of input ports configured to receive a data sequence comprising header information and payload information from an entity external to the cryptography accelerator (Fig, 4, items 401 or 412 and associated text describe a network interface which receives/sends data packets from/to the network); a plurality of cryptographic processing cores (Ziai teaches a cryptographic processing core, but does not explicitly indicate a **plurality** of cores. However, it would have been obvious to the one skilled in art to use multiple cryptographic cores to improve the speed of cryptographic processing. This is shown in Anad Fig. 1 and 2 and associated text, where a cryptographic core is shown to handle 4 independent channels. Fig. 2 item 208 also shows a buffer shared by input ports, which sends the packets from different channels for cryptographic processing (hashing) to the core. Also, col. 21 lines 47-52 clearly shows the option of multiple cores to perform cryptographic process to improve the speed. The combination of Anand's teaching of multiple input ports and

cryptographic cores with Ziai would have been obvious to the one skilled in art, because the two references are analogous art, and the motivation to combine would be to improve the speed of cryptographic process.); a shared input buffer associated with a plurality of input ports and the plurality of cryptographic processing cores, the shared input buffer configured to hold payload information associated with the data received by the plurality of input ports (Fig. 4, items 403 or 419 and associated text); and a security association lookup unit configured to identify a security association address in a first portion of the address space associated with the cryptography accelerator by using header information (col. 6, line 17-43), the first portion of the address space corresponding to bus controller memory wherein the security association lookup unit is operable to acquire the security association information from bus controller memory (the security association information is obtained from the IPSEC security association data base (item 420, Fig. 4), which works with the cryptographic accelerator (item 402 or 411) and is associated with the DMA controller. DMA controller takes control of the bus and memory for data transfer between devices).

5.2. As per claim 2, Ziai is directed to the cryptography accelerator of claim 1, wherein the security association lookup unit identifies the security association address using header information associated with the received data sequence (col. 6, line 4-10).

5.3. As per claim 3, Ziai is directed to the cryptography accelerator of claim 2, wherein the security association lookup unit identifies the security association address

by performing a hash on the header information (see response to claim 2, and note that hashing to create an index to identify the address of data located in memory was a standard and widely used procedure in database systems at the time of invention).

5.4. As per claim 4, Ziai is directed to the cryptography accelerator of claim 2, wherein the security association lookup unit identifies the security association address by performing a hash using a source address, a destination address, a SPI, a source port number, and a destination port number (see response to claim 2 and col. 6, lines 4-10).

5.5. As per claim 5, Ziai is directed to the cryptography accelerator of claim 4, wherein the hash further uses protocol information and a version number (per col. 6, line 4-10, the information used to determine the security association address is IP addresses. Therefore, the protocol data (IP) and its version (IP version 4 and IP version 6 have different addressing scheme) are part of information).

5.6. As per claim 6, Ziai is directed to the cryptography accelerator of claim 1, wherein the first portion of the address space is a HyperTransport address space (HyperTransport links connect devices in ICs. Item 415 in Fig. 4 is a link between IC devices, and is separate from the system bus (col. 7, line 65-70).

5.7. As per claim 7, Ziai is directed to the cryptography accelerator of claim 1, wherein the first portion of the address space is a Peripheral Components Interface (PCI) address space (Fig. 4 item 405 is a peripheral memory, with a peripheral address space).

5.8. As per claim 8, Ziai is directed to the cryptography accelerator of claim 7, wherein a second portion of the address space corresponds to a system memory address space, the random access memory coupled to a CPU external to the cryptography accelerator (Fig. 3A item 307 and associated text, which is a memory separate from the accelerator memory space).

5.9. As per claim 9, Ziai is directed to the cryptography accelerator of claim 8, wherein a third portion of the address space corresponds to on-chip memory (col. 4, line 62-66).

5.10. Claims 10 and 11 were cancelled by the applicant.

5.11. Limitations of claims 12-19 are substantially the same as limitations of claims 1-9 above, and noting that Ziai teaches processing the second packet without waiting for the result of the read request for the first packet. This is taught by Ziai in col. Line 1-3, where it is determined if the packet requires IPSec processing. Per col. 6 lines 4-16, packets that do not require IPSec processing may bypass the decryption process

performed by the accelerator, and therefore be processed without waiting for result of the packets in front of it that require IPSec processing and decryption. Ziai also teaches plurality of cryptographic processing data paths as required by claim 13. As shown in col. 6 lines 17 to col. 7 line 24, packets go through different paths based on their security policy needs. For example, packets with ESP mode have different processing requirements than those with AH protocol. Note that the purpose of Ziai's invention is to free up system resources from having to wait for the results, or perform the cryptographic process requirements, by deploying additional cryptographic accelerators.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

Examiner

Art Unit: 2132

Benjamin E. Lanier
Primary Examiner
AU 2132